UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/583,452	05/30/2000	Daniel R. Zaharris	M-8376-US	1693

32605 7590 06/26/2008

MACPHERSON KWOK CHEN & HEID LLP
2033 GATEWAY PLACE
SUITE 400
SAN JOSE, CA 95110

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
06/26/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/583,452	ZAHARRIS ET AL.	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *04 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 6-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 6-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 06/04/2008.

2. Claims 1, 2 and 6-21 pending.

3. Claims 1 and 21 are amended.

Response to Arguments

Applicant's arguments have been fully considered but they are not persuasive.

1. Applicants on page 7 of the remarks argue that the media key of Bell is not private because the media key block is common to all the media and accessible by any hacker to hack the media key from the media key block. Examiner respectfully disagrees and asserts that although the applicants arguments are correct with respect to privacy of the media key block on the storage medium of the Bell system, but the amended claim 1 of the instant application does not recite any limitation to demonstrate that how the encryption/decryption core maintain the internal key private. Thus, combination of Bell and Scheidt meets the limitations of the claim 1.

2. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claim 1 as follows:

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 recites "wherein the encryption/decryption core is configured to maintain the internal key privately within the encryption/decryption core". This limitation makes the claim 1 indefinite because it merely claims the privacy of internal key but it does not state how the internal key remains private. Furthermore, it appears from claim 10 that the data stored on the storage medium has been encrypted by another entity different from the user system. This implies that the internal key is known by another system in another location and cannot be known and private only to the user system.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 6, 8, 9, 14, 16, 17, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bell et al. (6,832,319 B1; hereinafter Bell) in view of Scheidt (7,09,851 B1; Scheidt).

Referring to claim 1, Bell discloses:

a method for copying electronic data, once only, on a storage medium that includes a medium ID and media key block (abstract; col. 2, lines. 40-55) and Bell further discloses:

generating an internal key from a pseudo-random number within the data storage engine (col. 8, lines 62-col.9, line 10, where the media key corresponds to the recited internal key and the player-recorder corresponds to the recited data storage engine); generating a combination key by combining a medium key with the internal key within the data storage engine (Fig. 6; col. 7, lines 23-33, where the media identification corresponds to the recited medium key and the content key corresponds to the recited combination key which is generated within the player-recorder); and

wherein the encryption/decryption core is configured to maintain the internal key privately within the encryption/decryption core (see, for example, Fig. 6, where the steps of calculating media key, the content key and the decryption of data are carried out within the user system and the keys remain internal to the user system);

within the data storage engine, decrypting a first portion of data stored on the storage medium with said combination key (Fig. 6; col. 7, lines 23-33, where the content key corresponding to the recited combination key is used to decrypt the data read from the storage medium within the player-recorder).

Bell, however, does not expressly disclose:

generating a pseudo-random number within the data storage engine using a seed from a non-volatile memory.

Scheidt discloses a method for producing a cryptographic key by combining several components or splits, each of which may be provided by a different source (see, for example, abstract; col. 7, lines 20-30). Scheidt also discloses that a pseudo-random number is generated at both origin and destination spaces corresponding to the recited data storage engine (see, for example, col. 7, lines 32-41). Scheidt further discloses that the pseudo-random number is generated based on a seed value receiving from a source such a storage medium, floppy disk or a token corresponding to the recited non-volatile memory (see, for example, col. 4, lines 18-22; col. 7, lines 5-13; col. 7, lines 32-41; col. 7, lines 54-58). The calculated cryptographic key is used to decrypt the ciphertext data to plaintext data at the destination (col. 6, lines 57-67).

It would have been obvious to a person of ordinary skill in the art at the time of the invention was made to incorporate in the system of Bell a scheme for generating a pseudo-random number within the encryption/decryption engine (i.e., disk reproducing device or data storage engine) as taught in Scheidt, because it would make difficult for an unauthorized person to defeat the cryptography scheme and to decrypt the encrypted data (Scheidt, col. 3, lines 3-12).

Referring to claim 2, Bell discloses:

decrypting a master media key; and generating the medium key from the master media key (col. 9, lines 8-12, where medium key block corresponds to the recited master media key).

Referring to claim 6, Bell discloses:

The method of claim 1, wherein the combination key is generated by combining the internal key with the medium key in an exclusive OR function (col. 7, lines 59-62; col. 9, line 12-16).

Referring to claim 8, Bell discloses:

The method of claim 2 wherein the medium key comprises a mastered system area key, a writable system area key and a file system information key (Fig. 3; col. 6, lines 15-21).

Referring to claim 9, Bell discloses:

generating an additional internal key (col. 3, lines 25-50).

Referring to claims 14 and 20, Bell discloses:

generating a plurality of internal keys using a pseudo-random number generator (data storage engine) (see col. 3, lines 17-50; col. 8, line 59-col. 9, line 16);

decrypting a master media key and a file system structure corresponding to a first portion of the data using at least one internal key (see col. 7, lines 23-33; col. 9, lines 8-12, where medium key block corresponds to the recited master media key);

generating a plurality of medium keys from the master media key (see col. 3, lines 17-50; col. 8, lines 46-67);

generating a plurality of combination keys from the plurality of medium keys and the plurality of internal keys (see col. 4, lines 1-25; col. 7, lines 23-33, where the media identification corresponds to the recited medium key and the content key corresponds to the recited combination key which is generated within the player);

decrypting a first portion of the data using a first combination key (see col. 3, lines 25-30; col. 7, lines 23-33, where the content key corresponds to the recited combination key and it is used to decrypt the data read from the storage medium within the player); and

encrypting a first portion of data using said first combination key and storing the first portion on the storage medium (see col. 2, lines 50-55; col. 3, lines 8-16; col. 4, lines 1-8).

Bell, however, does not expressly disclose:

generating a pseudo-random number within the data storage engine using a seed from a non-volatile memory.

Scheidt discloses a method for producing a cryptographic key by combining several components or splits, each of which may be provided by a different source (see, for example, abstract; col. 7, lines 20-30). Scheidt also discloses that a pseudo-random number is generated at both origin and destination spaces corresponding to the recited data storage engine (see, for example, col. 7, lines 32-41). Scheidt further discloses that the pseudo-random number is generated based on a seed value receiving from a source such a storage medium, floppy disk or a token corresponding to the recited non-volatile memory (see, for example, col. 4, lines 18-22; col. 7, lines 5-13; col. 7, lines 32-

41; col. 7, lines 54-58). The calculated cryptographic key is used to decrypt the ciphertext data to plaintext data at the destination (col. 6, lines 57-67).
It would have been obvious to a person of ordinary skill in the art at the time of the invention to incorporate in the system of Bell a scheme for generating a pseudo-random number within the encryption/decryption engine (i.e., disk reproducing device or data storage engine) as taught in Scheidt, because it would make difficult for an unauthorized person to defeat the cryptography scheme and to decrypt the encrypted data (Scheidt, col. 3, lines 3-12).

Referring to claims 16, 17 and 19, Bell discloses that DVD disk may contain different encrypted data recorded in different area of the disk each section with its own associated key that is used for the encryption of data and the combination key for decryption (see, for example, col. 3, lines 25-50; col. 5, lines 33-53; col. 8, lines 38-67).

Claims 7, 10-13, 15, 18 and 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bell et al. (6,832,319 B1; hereinafter Bell) in view of Scheidt (7,09,851 B1; Scheidt) and further in view of Silverbrook et al. (6,334,190 B1; Silverbrook).

Referring to claims 7, 18 and 21, Bell in view Scheidt discloses that different data may be recorded on different area of a DVD disk and each portion of data encrypted and decrypted with particular keys using any type of cryptography technology

(see, for example, col. 3, lines 25-50; col. 5, lines 33-53; col. 8, lines 38-67). But Bell in view Scheidt does not expressly disclose the use of DES and triple DES for decryption and encryption. Silverbrook discloses the use of DES standard for encryption and decryption (col. 3, lines 64-67) and specifically the use of triple DES for more security (col. 4, lines 7-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to utilize triple DES for encryption and decryption instead of single DES as taught in Silverbrook in the system of Bell in view Scheidt, because it would provide a much higher level of protection and security for the secure data (col. 1, lines 25-31).

Referring to claims 10, 11 and 13, these claims are rejected as applied to the like elements of claims 1,4, 6 and 9 as stated above.

Referring to claim 12, Bell in view Scheidt discloses any number of different encrypted data can be recorded on the DVD disk (see, for example, col. 3, lines 25-50; col. 5, lines 33-53; col. 8, lines 38-67) and any cryptosystem type and encryption key can be applied to the recorded information (col. 1, lines 56-64).

Referring to claim 15, Bell in view Scheidt discloses the use of a pseudo-random number generator comprising a logical feedback shift register (LFSR) and a seed for the LFSR (see Scheidt, col. 8, lines 25-30; col. 9, lines 10-22; col. 16, lines 3-20).

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Abdulhakim Nobahar/

Examiner, Art Unit 2132

June 18, 2008

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132